A New World: Post-Pandemic Information Security Architecture

Dan Han
Virginia Commonwealth University

Agenda

- Review business operations and information security architecture in the past 20 years
- Discuss challenges leading up to the pandemic
- Discuss new challenges introduced during and following the pandemic
- Explore a different information security architecture that may help to address the current challenges
- Explore future security architectures that may function in the post-pandemic world

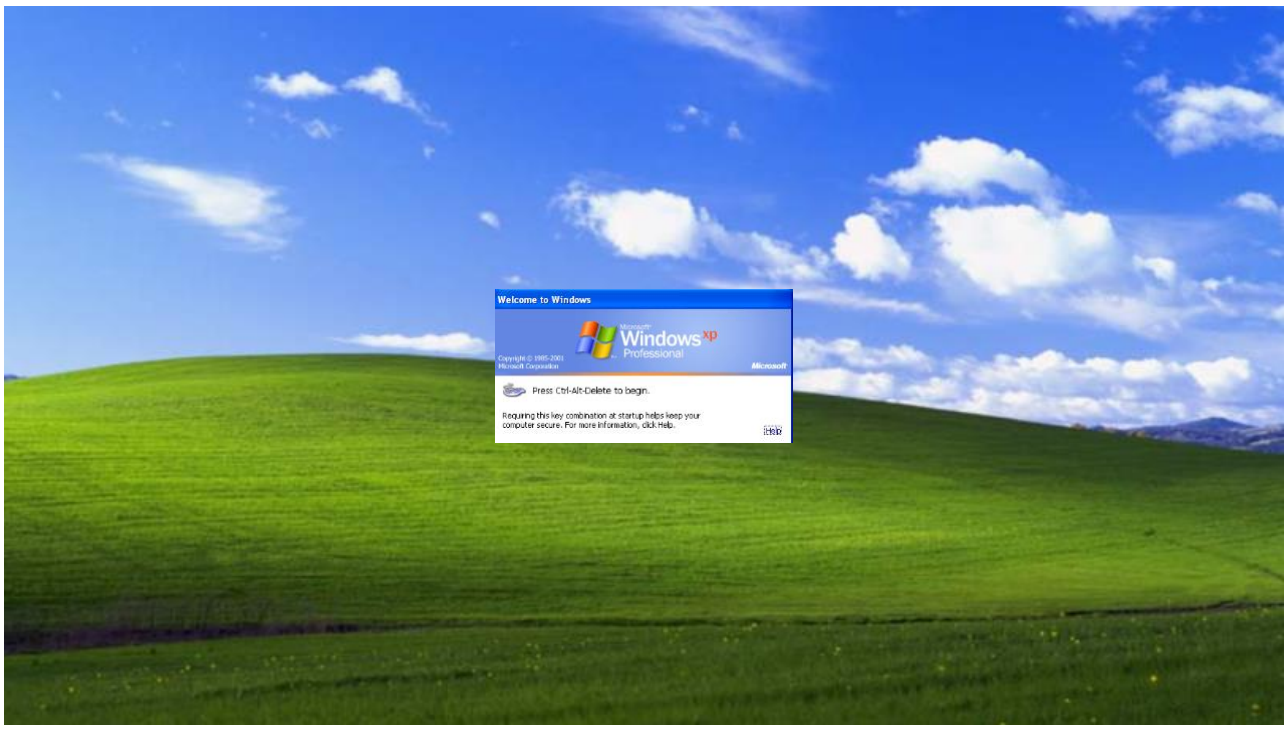
20 Years ago…


Playlists
Favorites
Monday Morning
Party Mix
Road Trip
Top 5 Break-Up Songs
Workout Tunes


WIKIPEDIA
The Free Encyclopedia


Sony Ericsson
Sony Ericsson


ADSL
Ethernet

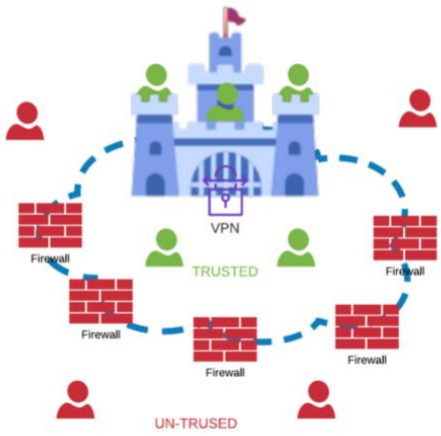

Welcome to Windows
Windows xp
Professional
Press Ctrl-Alt-Delete to begin.
Requires this key combination at startup helps keep your computer secure. For more information, click Help.

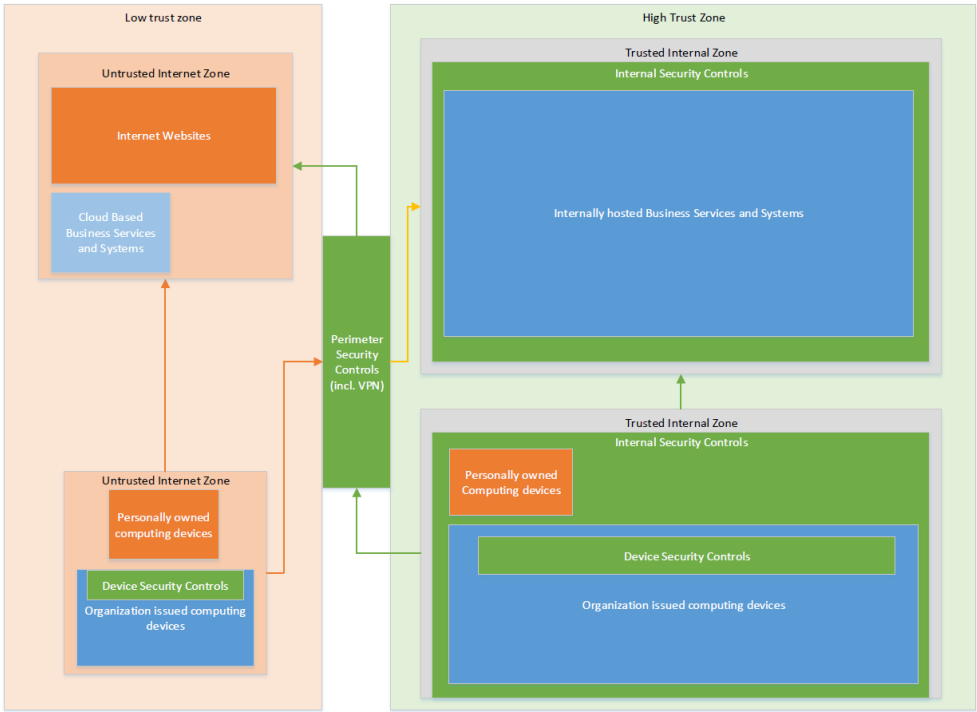
```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)


***  SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

Information Security became a thing

- Aside from the policies and procedures, we focused on
  - Antivirus
  - SPI Firewalls
  - IDS/IPS on plaintext traffic
  - QoS throttling
  - Some configuration management
  - VPNs
  - Saying “No” to the intellectually challenged users

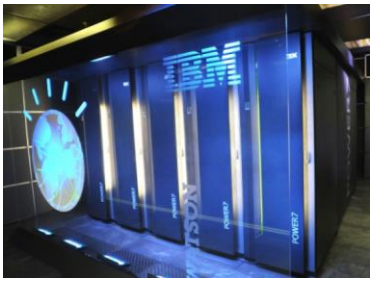
For the most part, we spent the next 10 years building moats around our castle

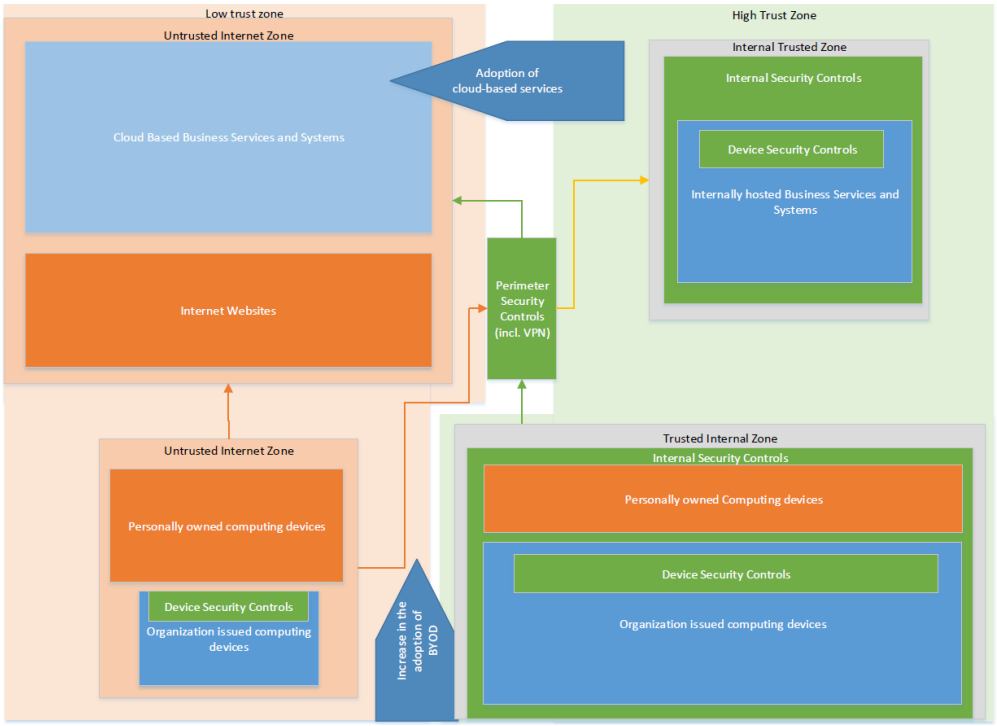




10 Years Ago…

amazon web services™

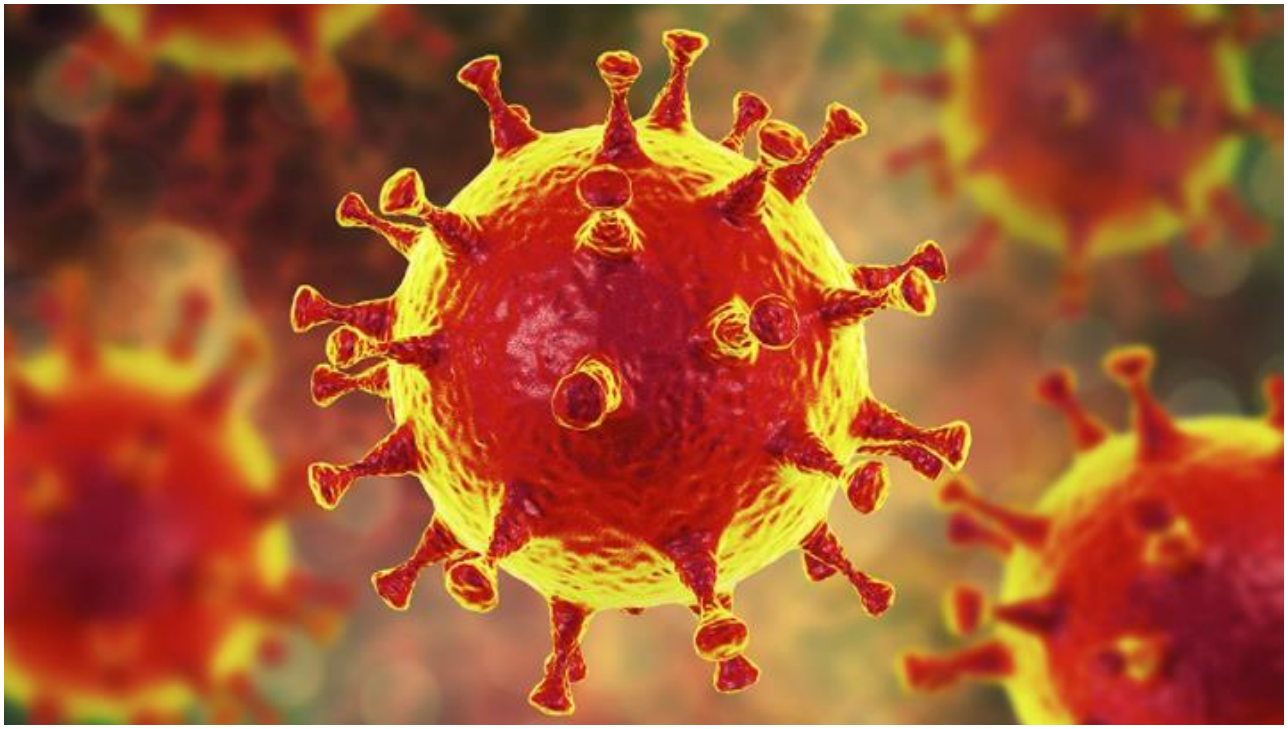




As such...

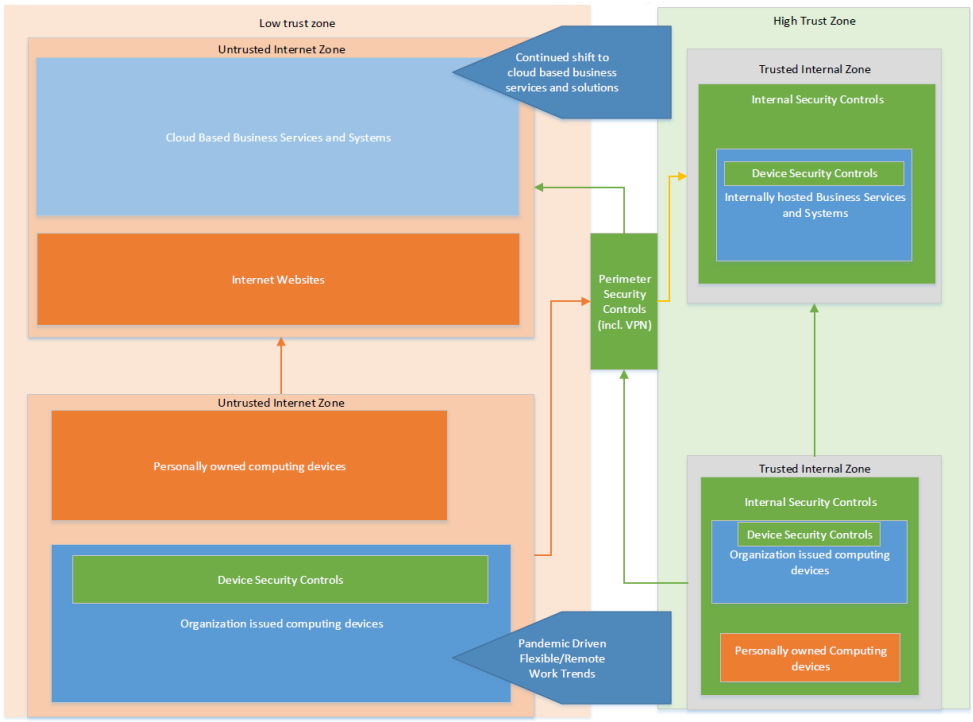
- The additional focus of security in the past 10 years
  - Mobile Device Management
  - Third-Party Risk Assessments
  - Enterprise Governance, Risk, and Compliance platforms
  - Advanced SIEM with UEBA
  - Layer 7 Firewalls with SSL/TLS inspection
  - Web App and workload protection
  - Cloud Access Service Brokers
  - Data Loss Prevention technologies

And then, between late 2019 to early 2020…



The current environment

- Anything-as-a-Service
- Bring Your Own Devices (BYOD)
- Bring Your Work Home (BYWH)



Compounding on top of this…

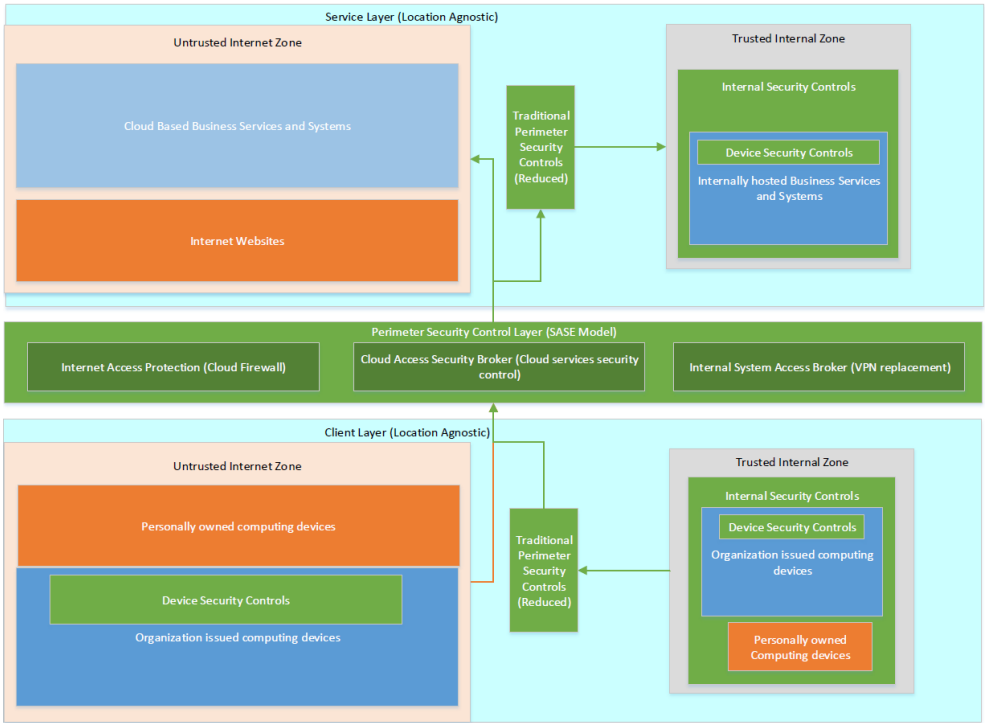
Fueled by the rise of Cryptocurrency…

- Sophistication in cybercriminal operations
  - Phishing-as-a-Service
  - Malware-as-a-Service
  - Ransomware-as-a-Service
  - Professional training services on committing cybercrime
  - Compromised access marketplaces
  - Tiered affiliation and contractor programs
  - Dedicated business analysis and target selection funtions
  - Professional HR units with talent recruitment services
  - Multi-factor Authentication Bypass

Therefore…

Rethinking our security architecture

- The great aspirations of business operational freedom
  - Work from anywhere
  - Work from any device
  - Work at any time



Components of a location agnostic model

- Firewall-as-a-Service (FWaaS) or Internet Access Protection (IAP)
  - Location-agnostic L7 Firewall, IDS/IPS, SWG, and sometimes, DLP
- Private Access Broker (PAB)
  - Always on remote access to internal resources
  - Posture checking for access

Components of a location agnostic model

- Cloud Access Security Broker (CASB)
  - Not new, but much more capable now than before.
  - Ability to govern individual use of cloud applications.
- Advanced AV and EDR
  - Can help to further strengthen individual endpoint devices.

Other tools of SASE

- Browser Isolation
  - A “remotely delivered secured browser” that can safeguard individual client computers and mobile devices against browser based exploits.
- DLP
  - The traditional data-loss-prevention, or more likely data-loss-detection tool that can monitor data leakage
- TLS inspection
  - Allows detection and prevention of threats sitting in TLS tunnels, but certificate management may still be an issue.

Considerations

- Cost
  - Bundled or A-la-carte model. Can be expensive
  - Almost entirely Opex based
- May still need some on-prem deployments
  - Log collection into SIEM
  - Private access broker system
  - IAM integration
  - Continued need of a minimized traditional on-prem stack
- Human capital
- Privacy
- Back to basics configuration management

Possible Alternative

- Full-tunnel VPN with existing security stack
  - Ensure VPN is enabled at all times when device is on
  - Ensure VPN appliances can handle concurrent connections from your population and enough bandwidth is allocated
  - Possible use of separate profiles (i.e. do we want to provide full-tunnel for everyone)
  - Will leverage existing capabilities of your on-prem security stack.
  - May be much less expensive to implement.

- Considerations
  - Remote access from distant locations
  - Sub-optimal on-prem security stack
  - Additional complexity and management overhead
  - Potential single-point-of-failure if on-prem is down

What about device-agnostic access?

Current and possible solutions

- Current
  - Mobile device management tied to application access
    - Possible health checks before access to data is permitted
    - May be limiting access to specific applications
  - VPN connections with security posture checks
    - More advanced security posture checks
    - Helps with system access to systems that are behind VPN
  - Limited use of application virtualization
  - Limited use of virtual desktops

Possible solutions to consider in the future

- Possible
  - Windows 365 or Azure Virtual Desktop
    - Windows 365 – Comparably fixed cost, persistent VDI, MS manages expensive and requires specific management stack.
    - Azure Virtual Desktop (AVD) – Pay-as-you-go or multi-year deal, more complex but flexible. Can offer persistent or non-persistent (pooled) VDIs that may be more cost effective. Supports more management models.
  - Possibly a SASE FWaaS and PAB/VPN agent
    - Device health-checks
    - Some limited endpoint security capabilities
    - Restriction of access to sensitive systems
  - Reduce the access through traditional remote access mechanisms

In summary…

- The aspirations of business operation freedom:
  - Work from anywhere
  - Work from any device
  - Work at any time
- With existing solutions to address BYOD and cloud apps, the traditional security model may need to be altered to provide a consistent and location agnostic security protection to the organization.

Thank you, questions?